UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/806,668	03/23/2004	Russell Wayne Dellmo	GCSD-1573 (51395)	1171

74701 7590 05/29/2008

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST
255 S ORANGE AVENUE
SUITE 1401
ORLANDO, FL 32801

EXAMINER	
PAN, JOSEPH T	
ART UNIT	**PAPER NUMBER**
2135	

NOTIFICATION DATE	DELIVERY MODE
05/29/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

creganoa@addmg.com

Office Action Summary	Application No.	Applicant(s)	
	10/806,668	DELLMO ET AL.	
	Examiner	Art Unit	
	JOSEPH PAN	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 February 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on February 21, 2008 has been entered.

2. Applicant's response filed on January 28, 2008 has been carefully considered. Independent claims 1, 11, 21, 25, and 29 have been amended. Claims 1-36 are pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-7, 11-17, 21-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dhir et al. (U.S. Patent No. 7,142,557 B2), hereinafter "Dhir", in view of Cheng (U.S. Pub. No. 2003/0221034 A1), and further in view of Allmond et al. (U.S. Patent No. 5,754,552), hereinafter "Allmond".

Referring to claim 1:

i. Dhir teaches:

A cryptographic device comprising:

a cryptographic module and a communications module (see figure 8, elements 321 'encryption engine', 301 'wlan [i.e., wireless local area network] transceiver' of Dhir);

said cryptographic module comprising

a user Local Area Network (LAN) network interface (see figure 8, elements 325 'host bus interface', 326 'host device interface'; and figure 9, element 335 'LAN', of Dhir),

a cryptographic processor coupled to said user Local Area Network (LAN) network interface (see figure 8, element 321 'encryption engine' of Dhir), and

said communications module comprising

a network wireless LAN interface (see figure 8, element 301 'wlan [i.e., wireless local area network] transceiver' of Dhir), coupled to said cryptographic processor and switchable between wireless LAN modes (see column 3, lines 1-17 of Dhir).

However, Dhir does not specifically mention that the cryptographic module and the communication module are removably coupled. Neither does Dhir specifically mention a plurality of different connectors for coupling the cryptographic module to different network devices.

ii. Cheng teaches a add-on card for connecting to both wired and wireless networks, wherein Cheng discloses that "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

On the other hand, Allmond teaches a communication protocol detection system wherein Allmond discloses a plurality of different connectors for coupling the cryptographic module to different network devices (see figure 3; and column 10, line 61 - column 11, line 24 of Allmond).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cheng into the method of Dhir to make the communication module removable from the cryptographic device.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Allmond into the method of Dhir to use a plurality of different connectors for coupling the cryptographic module to different network devices.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Cheng into the system of Dhir to make the communication module removable from the cryptographic device, because "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

The ordinary skilled person would have been motivated to have applied the teaching of Allmond into the system of Dhir use a plurality of different connectors for coupling the cryptographic module to different network devices, because Dhir teaches a method for providing a multi-platform wireless local area network (see column 3, lines 1-2 of Dhir, emphasis added). Allmond teaches a networking device to automatically detecting and interconnecting network devices, each operating according to any one of a plurality of communication protocols (see column 1, lines 16-20 of Allmond, emphasis added). Therefore, Allmond's teaching could enhance Dhir's system.

Referring to claims 2, 12, 22, 26, 30:

Dhir, Cheng, and Allmond teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose that the network wireless LAN interface circuit is switchable to one of an access point (AP) mode, an infrastructure mode, and an ad-hoc mode (see figure 9; and column 3, lines 1-17 of Dhir).

Referring to claims 3, 13, 23, 27, 31:

Dhir, Cheng, and Allmond teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the connector (see figure 4, element 55A, 55B, 57A, 57B of Cheng).

Referring to claims 4, 14, 24, 28, 32:

Dhir, Cheng, and Allmond teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the Ethernet (see column 2, lines 18 of Dhir).

Referring to claims 5, 15, 33:

Dhir, Cheng, and Allmond teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the power (see page 3, paragraph [0030], lines 10-13 of Cheng).

Referring to claims 6, 16, 34:

Dhir, Cheng, and Allmond teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the encryption algorithm (see column 9, lines 19-20 of Dhir).

Referring to claims 7, 17, 35:

Dhir, Cheng, and Allmond teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the processor and the encryption circuit (see figure 8, elements 324 'baseband processor', 321 'encryption engine' of Dhir).

Referring to claims 10, 20:

Dhir, Cheng, and Allmond teach the claimed subject matter: a communications system (see claim 1 above). They further disclose the disabling (see column 3, line 35 of Allmond).

Referring to claim 11:

i. Dhir teaches:

A cryptographic device comprising:

a cryptographic module and a communications module (see figure 8, elements 321 'encryption engine', 301 'wlan transceiver' of Dhir);

said cryptographic module comprising

a user local area network interface (LAN) (see figure 8, elements 325 'host bus interface', 326 'host device interface'; and figure 9, element 335 'LAN', of Dhir),

a cryptographic processor coupled to said user LAN interface (see figure 8, element 321 'encryption engine' of Dhir), and

said communications module comprising

a network wireless LAN interface (see figure 8, element 301 'wlan [i.e., wireless local area network] transceiver' of Dhir), and

said communications module comprising a predetermined one from among a plurality of interchangeable communications modules, and said network wireless LAN interfaces of said plurality of interchangeable communications modules each operating using a different wireless LAN mode (see column 3, lines 1-17 of Dhir).

However, Dhir does not specifically mention that the cryptographic module and the communication module are removably coupled. Neither does Dhir specifically mention a plurality of different connectors for coupling the cryptographic module to different network devices.

ii. Cheng teaches a add-on card for connecting to both wired and wireless networks, wherein Cheng discloses that "The network connection module can be detachable from the

add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

On the other hand, Allmond teaches a communication protocol detection system wherein Allmond discloses a plurality of different connectors for coupling the cryptographic module to different network devices (see figure 3; and column 10, line 61 - column 11, line 24 of Allmond).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cheng into the method of Dhir to make the communication module removable from the cryptographic device.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Allmond into the method of Dhir to use a plurality of different connectors for coupling the cryptographic module to different network devices.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Cheng into the system of Dhir to make the communication module removable from the cryptographic device, because "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

The ordinary skilled person would have been motivated to have applied the teaching of Allmond into the system of Dhir use a plurality of different connectors for coupling the cryptographic module to different network devices, because Dhir teaches a method for providing a multi-platform wireless local area network (see column 3, lines 1-2 of Dhir, emphasis added). Allmond teaches a networking device to automatically detecting and interconnecting network devices, each operating according to any one of a plurality of communication protocols (see column 1, lines 16-20 of Allmond, emphasis added). Therefore, Allmond's teaching could enhance Dhir's system.

Referring to claim 21:

i. Dhir teaches:

A communications method comprising:

coupling a cryptographic module to a Local Area Network (LAN) device, a cryptographic processor coupled to the user LAN interface (see figure 8, element 321 'encryption engine'; and figure 9, element 335 'LAN', of Dhir);

providing a communications module, a network wireless LAN interface (see figure 8, element 301 'wlan [i.e., wireless local area network] transceiver', of Dir);

using the network wireless LAN interface to communicate with a wireless LAN (see column 6, line 66-column 7, line 3 of Dhir).

However, Dhir does not specifically mention that the cryptographic module and the communication module are removably coupled. Neither does Dhir specifically mention a plurality of different connectors for coupling the cryptographic module to different network devices.

ii. Cheng teaches a add-on card for connecting to both wired and wireless networks, wherein Cheng discloses that "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

On the other hand, Allmond teaches a communication protocol detection system wherein Allmond discloses a plurality of different connectors for coupling the cryptographic module to different network devices (see figure 3; and column 10, line 61 - column 11, line 24 of Allmond).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cheng into the method of Dhir to make the communication module removable from the cryptographic device.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Allmond into the method of Dhir to use a plurality of different connectors for coupling the cryptographic module to different network devices.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Cheng into the system of Dhir to make the communication module removable from the cryptographic device, because "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

The ordinary skilled person would have been motivated to have applied the teaching of Allmond into the system of Dhir use a plurality of different connectors for coupling the cryptographic module to different network devices, because Dhir teaches a method for providing a multi-platform wireless local area network (see column 3, lines 1-2 of Dhir, emphasis added). Allmond teaches a networking device to automatically detecting and interconnecting network devices, each operating according to any one of a plurality of communication protocols (see column 1, lines 16-20 of Allmond, emphasis added). Therefore, Allmond's teaching could enhance Dhir's system.

Referring to claim 25:

i. Dhir teaches:

A communications method comprising:

coupling a cryptographic module to a Local Area Network (LAN) device, a cryptographic processor coupled to the user LAN interface; coupling the user LAN interface to a LAN device (see figure 8, element 321 'encryption engine'; and figure 9, element 335 'LAN', of Dhir);

coupling one of a plurality of communication modules to the cryptographic module, and the network wireless LAN interfaces of the plurality of interchangeable communications modules each operating in a different wireless LAN mode (see figure 8, element 321 'encryption engine', element 301 'wlan [i.e., wireless local area network]; column 3, lines 1-17; and column 6, line 66-column 7, line 3 of Dhir); and

using the communications module to communicate with a wireless LAN (see figure 8, element 301 'wlan [i.e., wireless local area network]; and column 6, line 66-column 7, line 3 of Dhir).

However, Dhir does not specifically mention that the cryptographic module and the communication module are removably coupled. Neither does Dhir specifically mention a plurality of different connectors for coupling the cryptographic module to different network devices.

ii. Cheng teaches a add-on card for connecting to both wired and wireless networks, wherein Cheng discloses that "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

On the other hand, Allmond teaches a communication protocol detection system wherein Allmond discloses a plurality of different connectors for coupling the cryptographic module to different network devices (see figure 3; and column 10, line 61 - column 11, line 24 of Allmond).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cheng into the method of Dhir to make the communication module removable from the cryptographic device.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Allmond into the method of Dhir to use a plurality of different connectors for coupling the cryptographic module to different network devices.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Cheng into the system of Dhir to make the communication module removable from the cryptographic device, because "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

The ordinary skilled person would have been motivated to have applied the teaching of Allmond into the system of Dhir use a plurality of different connectors for coupling the cryptographic module to different network devices, because Dhir teaches a method for providing a multi-platform wireless local area network (see column 3, lines 1-2 of Dhir, emphasis added). Allmond teaches a networking device to automatically detecting and interconnecting network devices, each operating according to any one of a plurality of communication protocols (see column 1, lines 16-20 of Allmond, emphasis added). Therefore, Allmond's teaching could enhance Dhir's system.

Referring to claim 29:

i. Dhir teaches:

A communications system comprising:

a plurality of Local Area Network (LAN) devices coupled together to define a network, and a cryptographic device coupled to at least one of said LAN devices (see figure 9, element 335 'LAN'; and figure 8, element 321 'encryption engine', of Dhir);

said cryptographic device comprising a cryptographic module coupled to said at least one LAN device, and a communications module (see figure 8, element 321 'encryption engine', element 301 'wlan [i.e., wireless local area network] transceiver' of Dhir);

said cryptographic module comprising a cryptographic processor coupled to said user LAN interface (see figure 8, element 321 'encryption engine', element 325 'host bus interface', element 326 'host device interface' of Dhir);

said communications module comprising a network wireless LAN communications interface, coupled to the cryptographic processor and switchable between wireless LAN modes (see figure 8, element 301 'transceiver'; and column 3, lines 1-17, of Dhir).

However, Dhir does not specifically mention that the cryptographic module and the communication module are removably coupled. Neither does Dhir specifically mention a plurality of different connectors for coupling the cryptographic module to different network devices.

ii. Cheng teaches a add-on card for connecting to both wired and wireless networks, wherein Cheng discloses that "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

On the other hand, Allmond teaches a communication protocol detection system wherein Allmond discloses a plurality of different connectors for coupling the cryptographic module to different network devices (see figure 3; and column 10, line 61 - column 11, line 24 of Allmond).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cheng into the method of Dhir to make the communication module removable from the cryptographic device.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Allmond into the method of Dhir to use a plurality of different connectors for coupling the cryptographic module to different network devices.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Cheng into the system of Dhir to make the communication module removable from the cryptographic device, because "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

The ordinary skilled person would have been motivated to have applied the teaching of Allmond into the system of Dhir use a plurality of different connectors for coupling the cryptographic module to different network devices, because Dhir teaches a method for providing a multi-platform wireless local area network (see column 3, lines 1-2 of Dhir, emphasis added). Allmond teaches a networking device to automatically detecting and interconnecting network devices, each operating according to any one of a plurality of communication protocols (see column 1, lines 16-20 of Allmond, emphasis added). Therefore, Allmond's teaching could enhance Dhir's system.

5. Claims 8-10, 18-20, 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dhir et al. (U.S. Patent No. 7,142,557 B2) in view of Cheng (U.S. Pub. No. 2003/0221034 A1),

further in view of Allmond et al. (U.S. Patent No. 5,754,552), and further in view of Klein (U.S. Patent No. 6,857,076 B1).

Referring to claims 8, 18, 36:

i. Dhir, Cheng, and Allmond teach the claimed subject matter: a cryptographic device (see claim 1 above). Dhir further discloses the encryption engine (see figure 8, element 321 'encryption engine' of Dhir).

However, they do not specifically mention the data buffer.

ii. Klein teaches data security for digital data storage, wherein Klein discloses the data buffer (see column 5, lines 57-67 of Klein)

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Klien into the method of Dhir, Cheng and Allmond to utilize the data buffer for encryption.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Klien into the system of Dhir, Cheng and Allmond to utilize the data buffer for encryption, because data buffer can be used to store data during encryption process.

Referring to claims 9, 19:

Dhir, Cheng, Allmond, and Klein teach the claimed subject matter: a communications system (see claim 1 above). They further disclose the tampering (see column 7, line 44-45 of Klein).

Response to Arguments

6. Applicant's arguments, filed on January 28, 2008, have been fully considered. The amended independent claims now contain the claim limitation: "comprising a plurality of different connectors for coupling the cryptographic module to different network devices". Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Allmond.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Joseph Pan
May 21, 2008
/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135